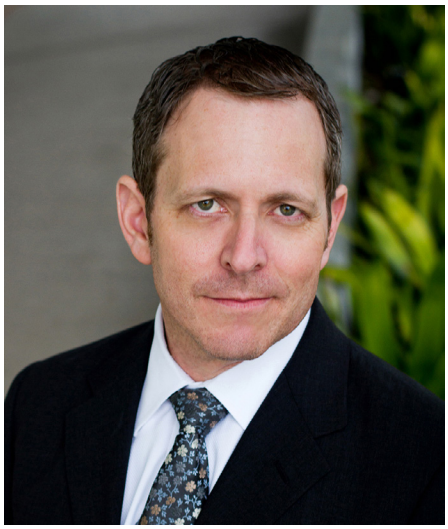
California Healthcare News®
cahcnews.com | Articles, Interviews and Statistics for the Healthcare Executive

# HIPAA – Society's Modern Day Prohibition

**By Craig B. Garner**
*Founder*
*Garner Health Law Corporation*



*"Secrets, silent, stony sit in the dark palaces of both our hearts: secrets weary of their tyranny: tyrants willing to be dethroned."*

James Joyce, *Ulysses*

***

Codified in American Law through Article Three of the United States Constitution and evolving through changing times by way of the Sixth and Fourteenth Amendments, the right to trial by jury remains a sacrosanct keystone of our nation's legal system. Even so, there exists a degree of delicacy with which the judicial system evaluates the facts of any given case, and all involved must remain mindful that at times pertinent information may not be available for consideration. Significant violations of judicial filtering may result in the end of deliberations, known more abrasively as a "mistrial."

The judicial system understands all too well that information cannot be honestly disregarded or ignored once heard, and does its best to account for the imperfections of the human mind. To enforce the Constitutional tenets of trust and truth upon which the faith of a jury must rest, today's health care providers find themselves held to a unique standard of scrutiny when dealing with issues of privacy.

Recently, the greatest challenge to health care in America has been to find ways in which to safeguard the confidentiality of patient health information, also known as protected health information (PHI). In the past several years, the United States has spent billions of dollars to safeguard the gamut of health information, from broken bones to heart surgery to mental illness, all of which are protected by federal and state law from public disclosure. The potential punishment for failure to respect and uphold patient confidentiality by those charged with its safekeeping strikes terror in those who may even unwittingly cause public disclosure.

The Federal Office of Civil Rights (OCR) oversees complaints relating to the 1996 Health Insurance Portability and Accountability Act (HIPAA), and more specifically those 109,722 HIPAA-related complaints registered between April 2003 and February 1, 2015. Of these potential HIPAA infractions, approximately 70% did not fall within OCR jurisdiction or the OCR determined no violation had occurred. But in some 40,000 cases investigated by the OCR, 30% found no violation, while 70% required some corrective action usually in reference to impermissible uses and disclosures of PHI, failure to keep PHI safe, lack of patient access to PHI, or disclosure of more information than was reasonably necessary. Private practices and acute care hospitals were among the worst offenders.

When it comes to PHI, the law of our nation insists that every

patient is entitled to absolute confidentiality. While the penalties for transgressions in confidentiality may differ due to a number of factors, health care's version of the proverbial mistrial is known collectively as a "data breach." In matters of health care records, however, not all data breaches are created equal, and perhaps more important, not all victims of a data breach are aware of the misuse of their information. Nevertheless, HIPAA's influence in this respect has changed the very infrastructure of health care, as it protects the disclosure of a broken finger as equally as a diagnosis of iatrophobia. It is important to note that, like stricken testimony or illegally obtained evidence, when sensitive medical information is divulged, the knowledge of its existence cannot be reversed.

As the new program flexed its muscles, it was no surprise that 2013 saw 6,381 more HIPAA complaints than 2004, resulting in a 51% increase over the decade. At times the complaints and resulting fines make sense, as when someone stumbled across the patient health information of a deceased partner, launching an investigation that ended in a $4.8 million fine against New York and Presbyterian Hospital and Columbia University. The fact that the transgression was caused by an errant physician deactivating a personal computer server on a system network did little to mitigate the record-breaking penalty levied against these two institutions. In terms of HIPAA, a breach is a breach.

Sometimes the penalty is appropriate, though it may not seem fair. One such example occurred when CBS purchased a photocopier from Affinity Health Plan, Inc. Before releasing the machine, Affinity forgot to delete the stored patient health information of up to 344,579 individuals. The resultant fine was $1,215,780.

There are also instances when a data breach determination is the right decision, even if the facts are somewhat at odds with the law. When a thief stole an unencrypted desktop computer from Sutter Health containing the patient information of over 4 million patients, one of the largest class actions to date followed. In 2014 the California Court of Appeal dismissed the 13 class action lawsuits seeking over $4 billion in damages because Sutter Health did not intend to disclose the compromised information, and the court ruled that loss of the unencrypted computer alone was "not a breach of confidentiality." When the California Supreme Court rejected this review, the health system's 50,000 employees, 5,000 physicians and 5,000 volunteer partners, not to mention the 197,264 patients discharged from Sutter Health in 2013, breathed a collective sigh of relief. While it would be tragic if a casual theft were to cause the insolvency of such a thriving system, California may never know what came of the 4 million missing patient records.

The right to an individual's privacy is by no means specific to the health care industry, but financial transgressions highlight the difficulty of protecting data in the modern age. While not necessarily a health record breach, Target's 2013 debacle affected 40 million credit and debit card accounts and exposed the data of 70 million customers. In 2012 Global Payments, Inc. reported the compromise of 1.4 million card accounts. Five million Tricare military beneficiaries took issue in 2011 when computer backup tapes with personal data on military service members went missing from the care of a Tricare-contractor. Finally, the February 2015 disclosure of a breach at Anthem involved as many as 80 million current and former Anthem members. With this in mind, perhaps the United States should take a different stand when it comes to HIPAA. With over 320 million residents to care for, we must ask ourselves how many mistrials and how many bells set into motion that cannot be unrung it will take before HIPAA proves itself unworthy of the task at hand? Only time will determine the future of HIPAA, though history tells us that the folly of prohibition lasted 13 years.

*Craig Garner is the founder of Garner Health Law Corporation, as well as a healthcare consultant specializing in issues pertaining to modern American healthcare. Craig is also an adjunct professor of law at Pepperdine University School of Law. He can be reached at craig@garnerhealth.com.*